

A moeda digital denominada Bitcoin é blindagem contra o reconhecimento da Lavagem de Capitais e da Evasão de Divisas?

por Marcos Carazai

A moeda digital denominada Bitcoin existe desde 2009 porém, ao longo, dos último três anos, o uso de Bitcoin cresceu substancialmente.

Para entender essa Moeda é imprescindível conhecer algumas questões básicas, vinculadas, principalmente, às operações da rede Bitcoin e sua interação com o atual sistema monetário.

O que é Bitcoin?

Bitcoin apareceu pela primeira vez em janeiro de 2009, a sua criação se deu por conta da atuação de um programador, o qual usou o pseudônimo Satoshi Nakamoto. Sua invenção é de código aberto e de exibição pública. Nas transações realizadas com Bitcoins (moeda Digital) não se exige um intermediário, como PayPal ou Visa.

Como o dólar dos EUA, o Bitcoin não tem valor intrínseco, pois não é resgatável, como uma onça de ouro. Ao contrário de um dólar, um Bitcoin não tem forma física, não é, totalmente, legal e seu fornecimento não é determinado por um banco central. O sistema Bitcoin é privado e conta com a atuação de algumas instituições financeiras tradicionais envolvidas em transações. Ao contrário das moedas digitais anteriores, que possuíam alguma pessoa ou entidade central, a rede Bitcoin é completamente descentralizada, tendo em todas as suas fases negociais, transações realizadas pelos usuários do sistema.

Como funciona o sistema Bitcoin?

O Bitcoin depende dos princípios da criptografia (comunicação segura) para validar transações e governar a produção da própria moeda. Cada Bitcoin e cada usuário são criptografados com uma identidade única, e cada transação é registrada em um livro

público descentralizado, que é visível por todos os computadores da rede, mas não é revelada nenhuma informação pessoal sobre o valor envolvido. Técnicas criptográficas permitem transações e a conferência, onde são verificadas se as transações são válidas, e ainda, é conferido se o comprador tem o montante de Bitcoin gasto e o transferiu para a conta do vendedor.

Essa gestão descentralizada, registrada em livro público é o atributo tecnológico distintivo do Bitcoin, porque soluciona o chamado problema de dupla despesa (ou seja, evita-se gastar dinheiro que não possui ou o uso de fraudes, por exemplo).

Como são obtidos Bitcoins?

Primeiro precisa ser baixada uma fonte livre e de código aberto, relacionada a mineração do Bitcoin. Uma vez conectado à rede, existem três maneiras de obter Bitcoins. Primeiro, um usuário pode trocar dinheiro convencional (por exemplo, dólares, reais, ienes e euros), pagando uma taxa, em um ambiente de troca online (por exemplo, Okcoin, Coinbase e Kraken). A taxa de câmbio cai com o tamanho da transação, variando de 0,5% para transações pequenas até 0,2% para grandes transações. O preço da Bitcoin em relação a outras moedas é determinado pela oferta e demanda. Em **segundo** lugar, um usuário pode obter Bitcoins em troca da venda de bens ou serviços, como quando um comerciante aceita Bitcoin de um comprador para a venda de seu produto. Em **terceiro** lugar, um usuário pode adquirir novos Bitcoins servindo como mineiro e aplicando o poder de processamento de seu computador ao verificar, com sucesso, a validade de novas transações de rede. A probabilidade de um indivíduo descobrir Bitcoins através da mineração é proporcional à quantidade de poder de processamento de computador que pode ser aplicada. Esta perspectiva provavelmente será muito pequena para o escritório típico ou o computador doméstico. O fornecimento de Bitcoins não depende da política monetária de um banco central virtual. A este respeito, apesar de ser uma moeda sem valor intrínseco, a operação do sistema Bitcoin é semelhante ao crescimento do dinheiro sob um padrão-ouro, embora historicamente a quantidade de ouro extraído fosse mais errática do que o crescimento da oferta de Bitcoins. Dependendo da perspectiva de alguém, este atributo da rede bitcoin pode ser uma virtude ou um vício.

As transações Bitcoins são anônimas?

As transações Bitcoin não são verdadeiramente anônimas. Um exemplo de uma transação anônima é uma troca de dinheiro entre dois estranhos. Nesse caso, nenhuma informação pessoal precisa ser revelada, nem precisa haver um registro da transação.

Por outro lado, uma transação não anônima, por exemplo, em uma compra *online* típica, onde é usado um cartão de crédito, há a necessidade da transação desencadear a validação, por um intermediário externo, a quem as identidades do comprador e do vendedor e informações relativas ao negócio perpetrado, são identificáveis e passíveis de registro.

Com uma transação Bitcoin, não existe intermediário externo. O comprador e o vendedor interagem diretamente e suas identidades são criptografadas e nenhuma informação pessoal é transferida de um para o outro. No entanto, ao contrário de uma transação totalmente anônima, há um registro de transação. Um registro de transação total de cada Bitcoin e a identidade criptografada do usuário de Bitcoin é mantida no razão pública. Por esta razão, as transações Bitcoin são pensadas para serem pseudo anônimas, não, totalmente, anônimas.

Devido ao livro público, pesquisadores descobriram que, usando análises sofisticadas do computador, as transações envolvendo grandes quantidades de Bitcoin podem ser rastreadas e afirmam que, se utilizadas as ferramentas atuais, autorizadas pela Legislação, seria possível obter muitas informações sobre as pessoas que movimentam Bitcoins, o que, em tese, não garante, absolutamente, o reconhecimento de que essas operações são blindagens a garantir que seus participantes ficarão ilesos do reconhecimento dos crimes de lavagem de capitais e da evasão de divisas, isso, certamente, limita a capacidade do sistema em manter, totalmente, anônimo, o seu usuário, ou seja, se a operação pode ser rastreada e seus operadores identificáveis, podem os mesmo ser responsabilizados pelos crimes que dessas operações decorram, desde que especialistas consigam quebrar a criptografia adotada, na operação realizada, a qual envolveu o uso da moeda Bitcoin.